State Estimation and Contingency Analysis of the Power Grid in a Cyber-Adversarial Environment

Robin Berthier[1], Rakesh Bobba[1], Matt Davis[2], Kate Rogers[1, 2], and Saman Zonouz[3]

[1]Information Trust Institute
University of Illinois at Urbana-Champaign
Urbana, IL, USA
{rgb, rbobba}@illinois.edu

[2]PowerWorld Corporation
Champaign, IL, USA
matt@powerworld.com,
krogers6@illinois.edu

[3]Department of Electrical and Computer Engineering
University of Miami
Miami, USA
s.zonouz@miami.edu

Abstract—**Contingency analysis is a critical activity in the context of the power infrastructure, because it provides a guide for resiliency and enables the grid to continue operating even in the case of failure. A critical issue with the current evolution of the power grid into a so-called smart grid is the introduction of cyber-security threats due to the pervasive deployment of communication networks and digital devices. In this paper, we introduce a cyber-physical security evaluation technique to take into account those threats. The goal of this approach is to augment traditional contingency analysis by not only planning for accidental contingencies but also for malicious compromises. This solution requires a new unified formalism to model the whole cyber-physical system including interconnections among the cyber and physical components. The system model is later used to assess potential impacts of both cyber and physical contingencies in order to prioritize prevention and mitigation efforts.**

Keywords-component; formatting; style; styling; insert (key words)

I. Introduction

State estimation and contingency analysis are the two most fundamental tools for monitoring the power system. State estimation is the process of fitting data coming in from sensors in the field to a system model and determining an estimate of the power system state. By its nature, state estimation depends on the communication infrastructure, commonly called the SCADA (system control and data acquisition) system. These systems are currently undergoing many changes as new sensors and communications infrastructure is being deployed as part of the smart grid initiative. Indeed, the smart grid becomes the perfect example of a large and complex cyber-physical system.

This complexity and the inter-connected nature of the power grid infrastructure introduce critical cyber security threats that can impact state estimation and contingency analysis at multiple levels. First, cyber attacks can breach the integrity of sensor_data required for state estimation. Second, adversaries can initiate incidents that are out of the scope of traditional reliability analysis, such as cascading failures that could not be caused by accident.

While the problem of detecting and mitigating cyber intrusions has been extensively studied over the past two decades in the context of traditional IT systems, the requirements and constraints of a cyber-physical system such as the smart grid are different and usually more stringent. For example, a lot of power grid components have timing requirements that prevent traditional security solution from being deployed. Moreover, the fact that cyber systems and power grid components are inter-connected creates a new set of dependencies for which the security community has currently a poor understanding. Recently, several attempts have been conducted to model and analyze the cyber-physical threats in an offline manner [1—4]; however, to the best of our knowledge, there has been no efficient online solution proposed for cyber-physical attack detection and contingency analysis.

In this work, we present a cyber-physical contingency analysis framework that takes into account cyber- and power-side network topologies, malicious cyber asset compromises and power component failures. In particular, during an offline process, the cyber network topology and global access control policies is analyzed automatically to generate a network connectivity map that represents a directed graph encoding inter-host accessibilities. The resulting connectivity map is then used to generate a Markovian state-based model of the power-grid in an online manner. At any time instance, the current security state can be estimated using the generated model and the triggered set of cyber-side intrusion detection sensor alerts. Using a new cyber-physical security index, the criticality level of any system state is measured and a ranked list of potential cyber and/or physical contingencies that needs to be taken care of in priority is produced.

II. Example

To illustrate our approach, we present preliminary results on the case study of a power grid infrastructure that is based on a real-world power control network. Figure 1 shows the cyber-side topology, i.e., power control network topology of the power grid. Figure 2 shows the physical power system topology. As illustrated in Figure 1, the computer systems (gray circles identified by IP addresses) are interconnected through routers (blue circles) and network firewalls (red circles). The network topology is an abstract version of a real-world power control network. It is initially assumed that the attackers reside on a remote computer system denoted by the node labeled *Internet* in Figure 1. Figure 2 shows how the power system generation and load buses are interconnected through transmission lines. We use the NetAPT network analysis tool to parse and analyze the access control policies of the network and generate automatically the power grid attack graph that enumerates all possible attack paths against cyber assets and physical power system components. The attack graph for this case study is shown in Figure 3. Each node in the attack graph represents a compromised or damaged cyber or physical asset within the power grid.

The graph from Figure 3 provides the structure on which we can run state estimation algorithms to assess, at each time instant, the current state of the power grid given the past sequence of measurements from power system sensors (e.g., phase measurement units) and the cyber side security sensors (e.g., intrusion detection systems). In addition, this graph can be used to empirically evaluate the impact of cyber-physical contingency by taking into account what the attackers could or would do from any state of the power grid. This structure provides the power system operators with an invaluable knowledge base regarding global impacts of various cyber network or power system contingencies that can assist the identification of the parts of the power grid that need to be the focus of protection and monitoring efforts.

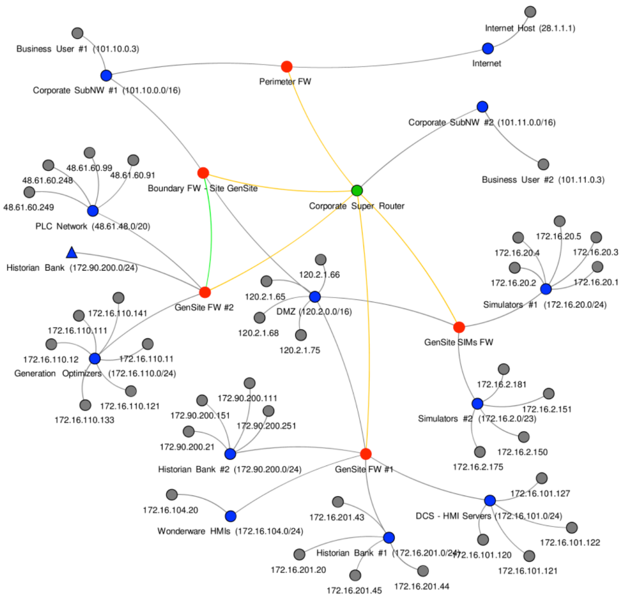

Figure 1: Control network configuration

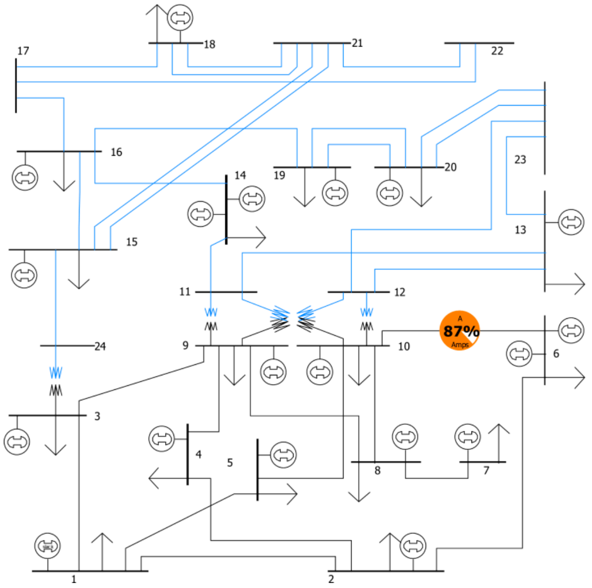

Figure 2: Power system topology

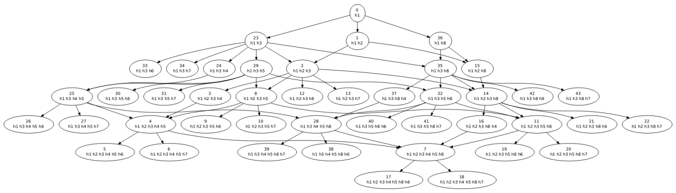

Figure 3: Attack graph

III. Conclusion

In summary, the main contribution of this work is to introduce a new framework for cyber-physical contingency analysis that addresses the challenge of state estimation of a complex and large-scale cyber-physical system. Next steps on this research 1) include the implementation and the evaluation of efficient state estimation algorithms that can cope with the large state space in a timely manner; 2) the introduction of a probabilistic solution to identify and ignore noisy or maliciously corrupted measurements among the sensory data; and 3) the capability to make predictions under high level of uncertainty.

References

[1] Thomas M Chen, Senior Member, Juan Carlos Sanchez-aarnoutse, and John Buford. Petri net modeling of cyber-physical attacks on smart grid. *Smart Grid IEEE Transactions on,* 2(99):1–9, 2011.

[2] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli. Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE,* 100(1):195 –209, jan. 2012.

[3] Fabio Pasqualetti, Florian Do ̈rfler, and Francesco Bullo. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. *CoRR,* abs/1103.2795, 2011.

[4] Siddharth Sridhar, Adam Hahn, and Manimaran Govindarasu. Cyber-physical system security for the electric power grid. *Proceedings of the IEEE,* 100(1):210–224, 2012.